

Serial No. 10/006,466  
Attorney Docket No. US018178  
Page 2 of 7

**Claims:**

Claim 1 (previously presented): A system for peer-to-peer access to a collection of data, comprising:

a musicbox implemented via at least one selected from the group consisting of a specialized musicbox device, specialized musicbox devices, a computer and computers, said musicbox comprising:

a persistent data store, the persistent data store containing a plurality of individually selectable data files of a predetermined data format, some of the data files being pre-loaded onto the persistent data store;

a data communications interface coupled to a data communications network to provide a peer-to-peer network, the data communications network comprising a plurality of musicboxes authorized to participate in the peer-to-peer network; and

a controller coupled to the persistent data store and the data communications interface; and

software stored in the musicbox and executable via the controller in the musicbox, wherein the software is configured to:

identify, without utilizing a central server, the plurality of authorized musicboxes executing instances of the software;

peer-to-peer share the data files with the identified authorized musicboxes, the sharing being restricted to the identified plurality of authorized musicboxes having authorization to participate in the peer-to-peer sharing of data files;

secure the data files from unauthorized access to prevent the data files from being retrieved in a perceptible format thereof by unauthorized musicboxes;

reproduce the data files into a predetermined perceptible format; and

provide authorized musicboxes access to use the data files, wherein to identify comprises:

detecting whether another system is executing an instance of software that allows and restricts peer-to-peer sharing of the data files; and

Serial No. 10/006,466  
Attorney Docket No. US018178  
Page 3 of 7

identifying said another system as an unauthorized musicbox not being a peer in response to a detection that said another system is not executing said instance.

**Claim 2 (previously presented):** The system of claim 1, wherein the data files comprise works subject to copyright and works not subject to copyright.

**Claim 3 (previously presented):** The system of claim 1, wherein the data files comprise at least one of audiovisual works, music recordings, performance recordings, digitized film recordings, digitized video recordings, graphic work images, text, and software.

**Claim 4 (currently amended):** A system for peer-to-peer access to a collection of data, comprising:

a musicbox implemented via at least one selected from the group consisting of a specialized musicbox device, specialized musicbox devices, a computer and computers, said musicbox comprising:

a persistent data store, the persistent data store containing a plurality of individually selectable data files of a predetermined data format, some of the data files being pre-loaded onto the persistent data store;

a data communications interface coupled to a data communications network to provide a peer-to-peer network; and

a controller coupled to the persistent data store and the data communications interface; and

software stored in the musicbox and executable via the controller in the musicbox, wherein the software is configured to:

identify other musicboxes executing instances of the software;

peer-to-peer share the data files with the identified other musicboxes, the sharing being restricted to the identified other musicboxes having authorization to participate in the peer-to-peer sharing of data files;

Serial No. 10/006,466  
Attorney Docket No. US018178  
Page 4 of 7

secure the data files from unauthorized access;  
reproduce the data files into a predetermined perceptible format; and  
provide authorized musicboxes access to use the data files, wherein said software is configured to secure data files from unauthorized access by selecting from among at least:

securing the data files to prevent the data files from being retrieved in the predetermined perceptible format by unauthorized musicboxes; and

securing the data files ~~to enable the data files to be~~ retrievable retrieved in the predetermined perceptible format by authorized musicboxes,

wherein to identify comprises:

detecting whether another system is executing an instance of software that allows and restricts peer-to-peer sharing of the data files; and

identifying said another system as an unauthorized musicbox not being a peer in response to a detection that said another system is not executing said instance.

**Claim 5 (currently amended):** The system of claim 4, further comprising an audio-visual interface, the audio-visual interface configured to export at least one selected from the group consisting of audio data and visual data ~~for usable in~~ further reproduction of content within the data files.

**Claim 6 (canceled)**

**Claim 7 (previously presented):** The system of claim 4, further comprising a central server to provide registration services, the central server being a peer participant in the peer-to-peer network.

**Claim 8 (previously presented):** The system of claim 4, further comprising an authorization device, wherein the authorization device comprises at least one of an electronic smart

Serial No. 10/006,466  
Attorney Docket No. US018178  
Page 5 of 7

card, a mechanical smart card, and an optical key smart card.

**Claims 9-20 (canceled)**

**Claim 21 (previously presented): A system for peer-to-peer access to a collection of data, comprising:**

means for storing persistent data, the persistent data comprising a plurality of data files of a predetermined data format, the data files further being secured from unauthorized access;

means for data communications, coupled to the means for storing persistent data; and

means for accessing the persistent data in communication with the means for storing persistent data and the means for data communications, wherein the means for storing persistent data, the means for data communications, and the means for accessing the persistent data are together implemented via a musicbox, wherein the musicbox comprises at least one selected from the group consisting of a specialized musicbox device, specialized musicbox devices, a computer and computers, wherein the means for accessing the persistent data is executable via a controller in the musicbox and configured to:

identify, without utilizing a central server, other systems executing the means for accessing the persistent data;

peer-to-peer share the persistent data with the identified other systems, the sharing being restricted to the identified other systems to prevent the persistent data from being retrieved in the predetermined data format by an unidentified system; and

provide identified systems access to use the persistent data, wherein to identify comprises:

detecting whether the other system is executing an instance of software that allows and restricts peer-to-peer sharing of the plurality of data files; and

identifying the other system as the unidentified system not being a peer in

Serial No. 10/006,466  
Attorney Docket No. US018178  
Page 6 of 7

response to a detection that said other unidentified system is not executing said instance.

**Claim 22 (canceled)**

**Claim 23 (previously presented): The system of claim 21, wherein said system does not include a central server.**

**Claim 24 (canceled)**

**Claim 25 (previously presented): The system of claim 1, wherein said system does not include a central server.**

**Claim 26 (currently amended): The system of claim 4, wherein said software is further configured to:**

secure a predetermined collection of data files to prevent unauthorized copying by unauthorized musicboxes, and

secure a predetermined collection of data files to enable authorized access to be retrievable by authorized musicboxes.